Cybersecurity Incident Report

Step 1

Section 1: Identify the type of attack that may have caused this network interruption
Section 1: Network Traffic Analysis DoS attack - SYN Flooding **Patterns in Logged Network Traffic:** 1. **Volume of TCP SYN Requests**: The network traffic logs show a substantial and abnormal increase in TCP SYN packets originating from an unfamiliar IP address. This is characterized by an unusually high frequency of SYN requests compared to normal traffic patterns. 2. **Half-Open Connections**: The logs indicate that the server is experiencing a high number of half-open TCP connections. These are connections that have received a SYN request but have not completed the three-way handshake, leading to a backlog. 3. **Consistent Source IP**: The SYN requests are predominantly coming from a single IP address or a small set of IP addresses, which is atypical for legitimate traffic and suggests a focused attack. **Analysis and Conclusion:** The observed patterns—specifically the overwhelming number of TCP SYN packets, the accumulation of half-open connections, and the concentrated source IPs—indicate that the network is experiencing a **SYN flood attack**. This type of attack involves flooding the server with a large volume of SYN requests to exhaust its resources and prevent it from establishing legitimate connections. The server's inability to complete the TCP handshake process for legitimate users results in the observed connection timeout errors and significant performance degradation of the website.

Section 2: Explain how the attack is causing the website to malfunction

When website visitors try to establish a connection with the web server, a **three-way handshake** using the TCP protocol occurs, consisting of these steps:

1. **SYN (Synchronize)**: The client sends a SYN packet to the server to initiate a connection and request synchronization.
2. **SYN-ACK (Synchronize-Acknowledge)**: The server responds with a SYN-ACK packet, acknowledging the client's request and sending its own synchronization request.
3. **ACK (Acknowledge)**: The client completes the handshake by sending an ACK packet, confirming receipt of the server's response and finalizing the connection.

When a malicious actor sends a large number of SYN packets all at once, the server is overwhelmed with connection requests. It begins to allocate resources to handle these requests but is unable to complete the handshake process for all of them. This leads to an excess of half-open connections, where the server is waiting for the final ACK packets from the clients that never arrive.

The logs indicate a high volume of SYN packets from an unfamiliar IP address, suggesting a SYN flood attack. This causes the server to become bogged down, unable to process legitimate connection requests, and ultimately results in the website becoming unresponsive to visitors

Step 2
HOW TO READ A WIRESHARK TCP/HTTP LOG

Step 3

Types of Network Attacks: I am familiar with different types of network attacks, including:

1. Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks, which aim to disrupt or deny access to network services. You also understand other attacks such as
2. Man-in-the-Middle (MitM) attacks, where attackers intercept and potentially alter communications between two parties, and Phishing attacks, which trick individuals into disclosing sensitive information.

Attack Mechanisms:

1. SYN flood attack, attackers overwhelm a server with a flood of SYN requests, leading to resource exhaustion and service unavailability.
2. MitM attack, attackers can intercept and manipulate data being exchanged between two parties, compromising confidentiality and integrity.

Detection and Mitigation: You are aware of various methods for detecting and mitigating network attacks.

1. packet sniffers to monitor and analyze network traffic, implementing firewalls and intrusion detection systems (IDS) to block malicious traffic, and employing rate-limiting and other techniques to manage and control incoming traffic.

Incident Response: You understand the importance of a quick and effective incident response to network attacks. This involves identifying the attack, containing its impact, and taking steps to recover from the incident, such as taking affected systems offline, applying patches, and strengthening defenses to prevent future occurrences.

- **SYN flood attack**.
- In a SYN flood attack, an attacker sends a large number of TCP SYN packets to a server with the intent to overwhelm it. This flood of connection requests causes the server to become bogged down as it tries to handle these requests, which leads to resource exhaustion. As a result, the server becomes unable to process legitimate connection attempts, causing the website to become unresponsive and resulting in connection timeout errors for users.
- In this case, the packet sniffer revealed a high volume of SYN requests from an unfamiliar IP address, further confirming the presence of a SYN flood attack. This overwhelming traffic is causing the server to lose its ability to respond to both the malicious traffic and legitimate user requests.

A **Denial of Service (DoS)** attack comes from a single source, overwhelming a target with excessive traffic or requests to make it unusable.

A **Distributed Denial of Service (DDoS)** attack involves many sources, often from a network of compromised computers (a botnet), working together to flood the target. This makes the attack much larger and harder to stop compared to a DoS attack.

The website is taking a long time to load and reporting a connection timeout error because it is likely under a **SYN flood attack**. In this type of attack, an attacker sends a massive number of TCP SYN requests to the server, overwhelming its resources. The server becomes bogged down by the high volume of requests and is unable to process legitimate connection attempts, leading to delays and ultimately causing connection timeout errors for users trying to access the site.